Case Study : Web cookies

Yahoo!

Data Breach

Company Description

Company Information:

Industry: Online Services
Valuation: $7.4billion (2020)
Employee: 8,600 (2017)
Location: United States

- **Yahoo!** is an American webservice provider. It is headquartered in Sunnyvale California and operated by the namesake company Yahoo Inc., which is 90% owned by investment funds managed by Apollo Global Management and 10% by Verizon Communications
- It provides a web portal, search engine Yahoo Search, and related services, including My Yahoo!, Yahoo Mail, Yahoo News, Yahoo Finance, Yahoo Sports and its advertising platform, Yahoo! Native.
- Yahoo was established by Jerry Yang and David Filo in January 1994 and was one of the pioneers of the early Internet era in the 1990s
- Source: Wikipedia Yahoo! – Wikipedia In *Wikipedia*

Attack Category

Web cookies used to falsify login credentials

Description of the Attack :

Yahoo! reported that the late 2014 breach likely used manufactured **web cookies** to falsify login credentials, allowing hackers to gain access to any account without a password.

The unauthorized access stems from the 500 million account breach Yahoo disclosed in September. Yahoo first alluded last October to the sneaky **forged cookie** method hackers may have used.

The first reported data breach in 2016 had taken place sometime in late 2014, according to Yahoo the hackers had obtained data from over 500 million user accounts, including account names, email addresses, telephone numbers, dates of birth, hashed passwords, and in some cases, encrypted or unencrypted security questions and answers. Security experts noted that the majority of Yahoo!'s passwords used the ***bcrypt*** hashing algorithm, which is considered difficult to crack, with the rest using the older ***MD5*** algorithm, which can be broken rather quickly.

Risk Assessment Report

Learning Outcome:

Develop a cyber security risk mitigation strategy specific to the organization

1.0 Introduction

1.1 Purpose

- A Risk assessment should be done to determine vulnerabilities within the organization

1.2 Scope of the security risk assessment

- Specify what systems , networks and applications were reviewed as part of the security assessments.
- Determine the role and responsibilities of the team leaders.
- The cost of the security breach and the prevention of further breaches

1.3 Vulnerability sources

- The assessment team will use vulnerabilities sources to help identify potential vulnerabilities

Roles and Responsibilities

NIST Guidelines

Learning outcomes:

Project team should follow the guidelines outlined in the NIST Cybersecurity Framework

www.nist.gov/cyberframework

- Identify- Protect- Detect

- Respond- Recover

Role	Responsibilities
Risk or Project Manager	The Risk Manager identifies risks, verifies if the risk is internal or an external threat.
Integrated Project .Team	This team is responsible for identifying the risks, determining the impact, timing, and priority of the risks.
Risk Owner(s)	The risk owner determines which risks require mitigation and contingency plans. They perform a cost benefit analysis of the proposed strategies. They are also monitoring, controlling and updating the status of the risk.
Other Key Stakeholders	They assist in identifying and determining the context, consequence, impact, timing and priority of the risk.

Vulnerabilities

Vulnerability #1
Open redirect vulnerability in Athenz v1.8.24

Summary
It allowed remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a specially crafted page.

Vulnerability #2
Multiple stack-based buffer overflows in Yahoo! Messenger

Summary
It allowed remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via the (1) shortcut or (2) title keys in an emoticons.xml file.

Vulnerability #3
Yahoo! Japan Box (aka jp.co.yahoo.android.ybox) application 1.5.1 for Android does not verify X.509 certificates from SSL servers

Summary
This allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.

Vulnerability #4
Cross-site scripting (XSS) vulnerability in uploader.swf

Summary
allows remote attackers to inject arbitrary web script or HTML via the allowed Domain parameter

Costs & Prevention

Cost

- (Reuters) - Yahoo has struck a revised $117.5 million settlement with millions of people whose email addresses and other personal information were stolen in the largest data breach in history.

Prevention

- Verizon agreed to spend $306 million between 2019 and 2022 on information security, five times what Yahoo spent from 2013 to 2016. It also pledged to quadruple Yahoo's staffing in that area.
- Since the cyberattacks, Yahoo have invalidated the **forged cookies** used in the security breach. They cannot be used again.
- Yahoo have also set up a 2-step verification process. A one-time security code is sent by text to the user's mobile or generated by an application when someone logs in with the password. Without this code, the account cannot be accessed.

Conclusion

Yahoo!

There are also unanswered questions about when Yahoo found out about the attacks. Did it take them 2-3 years to fully understand the scale of the security breach? Or did they only come clean when law enforcement agencies became involved? And the other question is: if they are telling the truth about discovering the attacks, why did it take them so long to realize?
There was a significant change in Yahoo's reaction to the seriousness of the cyber-attacks, and it is quite puzzling. In September 2016, Yahoo 'urged' users to change their passwords. By December, Yahoo forced users to change their passwords.